

**Section I:**  
**AMENDMENT UNDER 37 CFR §1.121 to the**  
**CLAIMS**

1. (currently amended) A system for authenticating a client device requesting a session of service from a service provider, comprising:

at least two matching one-time pad cryptological tables, a first of which is stored in a client device, and a second of which is accessible by a service security server, each table having multiple entries, each entry including a field for a indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each row containing at least one One Time Pad [[pad]] value;

a code exchanger configured to receive for receiving a pad value from said client device by said service security server upon request for initiation of a service session;

a code comparator configured to determine for determining if said received One Time Pad [[pad]] value is marked as "used" or "unused" in said second table;

a service session grantor configured to grant said service request responsive to determination that said received One Time Pad [[pad]] value is unused, including changing said used indicator to a "used" state upon said grant of service; and

a client device reconfigurator configured adapted to challenge said user of said client device responsive to determining that said received One Time Pad [[pad]] value is marked as "used", and to replace said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge, completing authentication of said client device without the need for a service history counter.

2. (currently amended) The system as set forth in Claim 1 wherein:
  1. said one-time pad cryptological tables further comprise a sequence index;
  2. said code comparator is further configured to determine if said received One Time Pad [[pad]] value is a next unused pad according to said sequence indicators;
  3. said session grantor is configured to grant a session only if said received pad is a next expected One Time Pad [[pad]] value; and
  4. said client device reconfigurator is ~~adapted~~ configured to respond to said received One Time Pad [[pad]] value not being a next expected One Time Pad [[pad]] value.
3. (original) The system as set forth in Claim 1 wherein said code exchanger comprises at least one communications network selected from the group of a telephone network, a wireless data network, a Local Area Network, a Wide Area Network, and an Internet.
4. (currently amended) The system as set forth in Claim 1 wherein client device reconfigurator is ~~adapted~~ configured to challenge said user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.
5. (currently amended) The system as set forth in Claim 1 wherein:
  1. said one-time pad cryptological tables further comprise an expiration field for each entry;
  2. said code comparator is further configured to determine if said received pad is expired;
  3. said session grantor is configured to grant a session only if said received pad is unexpired; and
  4. said client device reconfigurator is ~~adapted~~ configured to respond to said received pad being expired.

6. (currently amended) The system as set forth in Claim 1 wherein said client device reconfigurator is ~~adapted~~ configured to replace said tables using a secure replacement method.
7. (original) The system as set forth in Claim 1 wherein said service session grantor is further configured to require a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".
8. (currently amended) A method for authenticating a client device requesting a session of service from a service provider, said method comprising the steps of:
  - providing at least two matching one-time pad cryptological tables, disposing a first of which in a client device, and disposing a second of which such that it is accessible by a service security server, each table having multiple entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each row containing at least one One Time Pad [[pad]] value;
  - receiving a One Time Pad [[pad]] value from said client device by said service security server upon request for initiation of a service session;
  - determining if said received One Time Pad [[pad]] value is marked as "used" or "unused" in said second table;
  - responsive to determination that said received One Time Pad [[pad]] value is unused, granting said service request and changing said used indicator corresponding to said One Time Pad [[pad]] entry in said second table to a "used" state; and
  - responsive to determining that said received One Time Pad [[pad]] value is marked as "used", challenging said user of said client device, and replacing said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge, completing authentication of said client device without the need for a service history counter.

9. (currently amended) The method as set forth in Claim 8 wherein:
  1. said step of providing one-time pad cryptological tables further comprises providing a sequence index field for each table entry;
  2. said step of determining if said received One Time Pad [[pad]] value is used comprises determining if said received One Time Pad [[pad]] is a next unused One Time Pad [[pad]] value according to said sequence indicators;
  3. said step of granting a session comprises granting a session only if said received One Time Pad [[pad]] value is a next expected pad value; and
  4. said step of challenging said user comprises challenging said user responsive to said received One Time Pad [[pad]] value not being a next expected pad value.
10. (currently amended) The method as set forth in Claim 8 wherein said step of receiving a One Time Pad [[pad]] value comprises receiving a One Time Pad [[pad]] value via at least one communications network selected from the group of a telephone network, a wireless data network, a Local Area Network, a Wide Area Network, and an Internet.
11. (original) The method as set forth in Claim 8 wherein said step of challenging a user comprises challenging a user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

12. (currently amended) The method as set forth in Claim 8 wherein:
  1. said step of providing one-time pad cryptological tables further comprises providing an expiration field for each entry;
  2. said step of determining if said received One Time Pad [[pad]] comprises determining if said received One Time Pad [[pad]] is expired;
  3. said step of granting a session comprises granting a session only if said received One Time Pad [[pad]] is unexpired; and
  4. said step of challenging a user and replacing said tables comprises challenging a user if said received pad is determined to be expired.
13. (original) The method as set forth in Claim 8 wherein said step of replacing said tables comprises using a secure replacement method to provide said replacement table to said client device.
14. (original) The method as set forth in Claim 8 wherein said step of granting a service session comprises a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".

15. (currently amended) An article of manufacture for authenticating a client device requesting a session of service from a service provider, comprising:

a computer readable medium suitable for encoding one or more software programs; and

one or more software programs configured to cause a processor to perform the steps of:

(a) providing at least two matching one-time pad cryptological tables, disposing a first of which in a client device, and disposing a second of which such that it is accessible by a service security server, each table having multiple entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each row containing at least one One Time Pad [[pad]] pad value;

(b) receiving a One Time Pad [[pad]] value from said client device by said service security server upon request for initiation of a service session;

(c) determining if said received One Time Pad [[pad]] value is marked as "used" or "unused" in said second table;

(d) responsive to determination that said received One Time Pad [[pad]] value is unused, granting said service request and changing said used indicator corresponding to said One Time Pad [[pad]] entry in said second table to a "used" state; and

(e) responsive to determining that said received One Time Pad [[pad]] value is marked as "used", challenging said user of said client device, and replacing said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge, completing authentication of said client device without the need for a service history counter.

16. (currently amended) The article as set forth in Claim 15 wherein:
  1. said software for providing one-time pad cryptological tables further comprises software for providing a sequence index field for each table entry;
  2. said software for determining if said received One Time Pad [[pad]] value is used comprises software for determining if said received pad is a next unused pad value according to said sequence indicators;
  3. said software for granting a session comprises software for granting a session only if said received pad value is a next expected pad value; and
  4. said software for challenging said user comprises software for challenging said user responsive to said received pad value not being a next expected pad value.
17. (currently amended) The article as set forth in Claim 15 wherein said software for receiving a One Time Pad [[pad]] value comprises software for receiving a One Time Pad [[pad]] value via at least one communications network selected from the group of a telephone network, a wireless data network, a Local Area Network, a Wide Area Network, and an Internet.
18. (previously presented) The article as set forth in Claim 15 wherein said software for challenging a user comprises software for challenging a user with one or more methods selected from the group of requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

19. (currently amended) The article as set forth in Claim 15 wherein:
  1. said software for providing one-time pad cryptological tables further comprises software for providing an expiration field for each entry;
  2. said software for determining if said received One Time Pad [[pad]] comprises software for determining if said received One Time Pad [[pad]] is expired;
  3. said software for granting a session comprises software for granting a session only if said received One Time Pad [[pad]] is unexpired; and
  4. said software for challenging a user and replacing said tables comprises software for challenging a user if said received One Time Pad [[pad]] is determined to be expired.
20. (previously presented) The article as set forth in Claim 15 wherein said software for replacing said tables comprises software for using a secure replacement method to provide said replacement table to said client device.
21. (previously presented) The article as set forth in Claim 15 wherein said software for granting a service session comprises software for performing a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".